THE p-ADIC ANALYTIC SUBGROUP THEOREM REVISITED

CLEMENS FUCHS AND DUC HIEP PHAM

Abstract. It is well-known that the Wüstholz' analytic subgroup theorem is one of the most powerful theorems in transcendence theory. The theorem gives in a very systematic and conceptual way the transcendence of a large class of complex numbers, e.g. the transcendence of π which is originally due to Lindemann. In this paper we revisit the p-adic analogue of the analytic subgroup theorem and present a proof based on the method described and developed by the authors in a recent related paper.

2010 Mathematical Subject Classification: 11G99 (14L10, 11J86)
Keywords: commutative algebraic groups, transcendence theory, p-adic numbers

1. Introduction

In the 1980's, Wüstholz formulated and proved the so-called analytic subgroup theorem which counts as one of the most striking and significant results in (complex) transcendental number theory and has many applications (see [1] or [9]). Roughly speaking, the theorem asserts that an analytic subgroup of a commutative algebraic group contains a non-trivial algebraic point if and only if it contains a non-trivial algebraic subgroup. The analytic subgroup theorem gives, as very special cases, the classical theorems of Hermite, Lindemann and Gelfond-Schneider. It also directly implies the deep results of Schneider, Baker, Masser, Coates, Lang, et altera. It is the most natural generalization in terms of the qualitative version of Baker's theorem on linear forms in logarithms of algebraic numbers.

If we replace the complex domain by the p-adic domain, a natural question one can now ask is "*How about a p-adic analogue of the analytic subgroup theorem?*". Recently, Matev formulated a p-adic analogue of the analytic subgroup theorem and gave a proof for the statement (see [7]) following more or less the proof of the classical analytic subgroup theorem. We owe a debt of gratitude to an anonymous referee for the observation that there is even an earlier reference: the statement has already been mentioned, without proof and in equivalent form, by Bertrand in [4] (see Remarque 2 on p. 37). In this paper we present our version of Matev's proof in more details based on the methods described and developed in a recent related paper by the authors (see [6]) and give some corollaries that follow.

2. The p-adic analytic subgroup theorem and some consequences

For the reader's convenience, we recall Wüstholz' analytic subgroup theorem in more details. Let G be a commutative algebraic group defined over $\overline{\mathbb{Q}}$ and $\mathfrak{g}$ the Lie algebra of G. The set of complex points $G(\mathbb{C})$ of G has naturally the structure of a complex Lie group whose Lie algebra $\mathfrak{g}_{\mathbb{C}}$ is the complex vector space $\mathfrak{g} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$. There is an analytic homomorphism, the so-called (complex) exponential map

$$\exp_G : \mathfrak{g}_{\mathbb{C}} \to G(\mathbb{C})$$

which is defined as follows. For $\xi \in \mathfrak{g}_{\mathbb{C}}$ there exists a unique homomorphism

$$\varphi_\xi : \mathbb{C} \to G(\mathbb{C})$$

such that its differential maps the vector field dt to ξ. We define

$$\exp_G(\xi) := \varphi_\xi(1).$$

Let $\mathfrak{b}$ be a subalgebra of $\mathfrak{g}$ and put $B := \exp_G(\mathfrak{b} \otimes_K \mathbb{C})$. Then B is a Lie subgroup of $G(\mathbb{C})$ and said to be an analytic subgroup of G. The following theorem is called the analytic subgroup theorem (see [1, Theorem 6.1]).

Theorem 2.1 (Wüstholz)**.** *Let $B \subseteq G(\mathbb{C})$ be an analytic subgroup of $G(\mathbb{C})$. Then $B(\overline{\mathbb{Q}}) := B \cap G(\overline{\mathbb{Q}})$ is non-trivial if and only if there exists a non-trivial algebraic subgroup $H \subseteq G$ defined over $\overline{\mathbb{Q}}$ such that $H(\mathbb{C}) \subseteq B$.*

This theorem gives a fundamental generalization of the qualitative version of Baker's theorem in terms of commutative algebraic groups. More precisely, the qualitative version of Baker's theorem is the special case when the underlying algebraic group is a torus. Furthermore, it also implies many interesting results in transcendence. To give an example we consider the simplest application of the analytic subgroup theorem, namely Lindemann's theorem: If α is any non-zero complex number then not both of α and e^α can be algebraic. In fact, assume the contrary that both α and e^α are algebraic. We consider the algebraic group $G = \mathbb{G}_a \times \mathbb{G}_m$, here $\mathbb{G}_a$ denotes the additive group and $\mathbb{G}_m$ denotes the multiplicative group as usual. Then G is defined over $\overline{\mathbb{Q}}$, and the Lie algebra of G is $\mathfrak{g} \cong \mathrm{Lie}(\mathbb{G}_a) \times \mathrm{Lie}(\mathbb{G}_m) \cong \mathbb{Q} \times \mathbb{Q}$. This gives $\mathfrak{g} \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$. The set of complex points of G is $G(\mathbb{C}) = \mathbb{C} \times \mathbb{C}^*$ and the exponential map is given by $\exp_G : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}^*, (z, w) \mapsto (z, e^w)$. Let $\Delta = \{(z, z) \in \mathbb{C} \times \mathbb{C}\}$ be the diagonal and let $B = \exp_G(\Delta)$ be the associated analytic subgroup. Then

$$(0, 1) \neq (\alpha, e^\alpha) = \exp_G(\alpha, \alpha) \in B(\overline{\mathbb{Q}}).$$

Hence there exists a non-trivial algebraic subgroup H defined over $\overline{\mathbb{Q}}$ of G such that $H(\mathbb{C}) \subseteq B$. It follows that $H(\mathbb{C}) = B$, i.e. B is an algebraic group. We deduce that the function e^z is an algebraic function, a contradiction. This shows Lindemann's theorem.

We now discuss the p-adic analytic subgroup theorem. Let F be a complete subfield of $\mathbb{C}_p$ containing $\overline{\mathbb{Q}}$, i.e. $F = \mathbb{C}_p$, and let G be a commutative algebraic group defined over $\overline{\mathbb{Q}}$. According to Section 3.1 there is the logarithm map

$$\log_{G(F)} : G(F)_f \to \mathrm{Lie}(G(F)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} F.$$

We denote by V_F the F-vector space $V \otimes_{\overline{\mathbb{Q}}} F$ and by $G_f(\overline{\mathbb{Q}})$ the set of algebraic points in $G(F)_f$, i.e. $G_f(\overline{\mathbb{Q}}) = G(F)_f \cap G(\overline{\mathbb{Q}})$. The p-adic analytic subgroup theorem reads as follows:

Theorem 2.2. *Let G be a commutative algebraic group of positive dimension defined over $\overline{\mathbb{Q}}$ and let $V \subseteq \mathrm{Lie}(G)$ be a non-trivial $\overline{\mathbb{Q}}$-linear subspace. For $\gamma \in G_f(\overline{\mathbb{Q}})$ with $0 \neq \log_{G(F)}(\gamma) \in V_F$ there exists an algebraic subgroup $H \subseteq G$ of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\mathrm{Lie}(H) \subseteq V$ and $\gamma \in H(\overline{\mathbb{Q}})$.*

Replacing G by its identity component G^0 if necessary, and noting that $\mathrm{Lie}(G) = \mathrm{Lie}(G^0)$, we may, without loss of generality, assume in the proof of Theorem 2.2 that G is connected.

As already mentioned above, the theorem has been obtained by Matev (see [7, Theorem 1]). However, we remark that his paper is still only available as a preprint and that our proof below has been worked out independently and roughly at the same time as Matev has obtained his one. Because of this we find it worth to present also our version of the result. The proof of the theorem will be given in Section 4.4 by using Proposition 2.5 below. We get the following corollaries of the theorem whose proof will also be given in Section 4.

Corollary 2.3. *Let G be a commutative algebraic group of positive dimension defined over $\overline{\mathbb{Q}}$ and T a non-empty subset of $G_f(\overline{\mathbb{Q}})$. Denote by $W \subseteq \mathrm{Lie}(G(F))$ the $\overline{\mathbb{Q}}$-vector space generated by all elements $\log_{G(F)}(\gamma)$ for $\gamma \in T$. Then there exists an algebraic subgroup H of G defined over $\overline{\mathbb{Q}}$ such that $\mathrm{Lie}(H) = W$.*

Corollary 2.4. *Let $\varphi : X \to G$ be a homomorphism of commutative algebraic groups defined over $\overline{\mathbb{Q}}$ with $\dim G > 0$ and $\varphi_F : X(F) \to G(F)$ the homomorphism of Lie groups over F induced by φ. If x is a point in $X(F)$ such that $\varphi_F(x)$ is a non-torsion point in $G_f(\overline{\mathbb{Q}})$, then there exists an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ satisfying:*

1. $\varphi_F(x) \in H$,
2. $\mathrm{Lie}(H) \subseteq \varphi_*(\mathrm{Lie}(X))$, *here* φ_* *is the tangent map induced by* φ.

To prove the p-adic analytic subgroup theorem, we shall reduce it to the semistable case (for the definition of semistability see Section 3.2; compare also with [7, Theorem 5] and [7, Lemma 6]). In this case we have the following proposition.

Proposition 2.5. *Let G be a commutative algebraic group defined over $\overline{\mathbb{Q}}$ of positive dimension and V a proper $\overline{\mathbb{Q}}$-linear subspace in* $\mathrm{Lie}(G)$, *i.e. V is non-trivial and $V \neq$* $\mathrm{Lie}(G)$, *such that (G, V) is semistable over $\overline{\mathbb{Q}}$. Then for any non-torsion point γ in $G_f(\overline{\mathbb{Q}})$ the element* $\log_{G(F)}(\gamma)$ *does not belong to V_F.*

The proposition plays a crucial role for proving Theorem 2.2, and the next sections up to Section 4.3 are devoted to prove it.

3. Preliminaries

3.1. **Exponential and logarithm map over p-adic fields.** Throughout this section, we denote by F a complete subfield of $\mathbb{C}_p$. Let G be a commutative algebraic group defined over F and $\mathrm{Lie}(G)$ its Lie algebra. It is known that the set of F-points has a structure of Lie group over F and its Lie algebra coincides with $\mathrm{Lie}(G)$. Furthermore, if $\varphi : G \to H$ is a homomorphism of commutative algebraic groups defined over F with the tangent map $\varphi_* : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$, then it induces a homomorphism of Lie groups over F from $G(F)$ to $H(F)$ whose differential map is φ_*. Recall that by [3, Chapter III, 7.6] there is a F-analytic homomorphism the so-called logarithm map $\log_{G(F)} : G(F)_f \to \mathrm{Lie}(G)$ where $G(F)_f$ is the set of $x \in G(F)$ for which there exists a strictly increasing sequence (n_i) of integers such that x^{n_i} tends to the unity element of $G(F)$ as i tends to ∞. One can show that $G(F)_f$ is an open subgroup of $G(F)$ such that the quotient group $G(F)/G(F)_f$ has no non-zero torsion elements. We also note that there is an open subgroup U of $\mathrm{Lie}(G)$ and a F-analytic homomorphism $\exp_{G(F)} : U \to \exp_{G(F)}(U) \subseteq G(F)_f$ such that $\exp_{G(F)}$ is the inverse map of the map which is the restriction of $\log_{G(F)}$ to $\exp_{G(F)}(U)$. In particular, this shows that $\log_{G(F)}(\gamma) = 0$ with $\gamma \in G(F)_f$ if and only if γ is a torsion point. We list below some important properties of logarithm maps (see [10]):
1. For commutative algebraic groups G, H defined over F, the logarithm map $\log_{(G\times H)(F)}$ is the map $\log_{G(F)} \times \log_{H(F)}$ with $(G \times H)(F)_f = G(F)_f \times H(F)_f$ and with $\mathrm{Lie}((G \times H)(F)) = \mathrm{Lie}(G(F)) \times \mathrm{Lie}(H(F))$.
2. For a homomorphism $\varphi : G \to H$ of commutative algebraic groups defined over F, the set $\varphi(G(F)_f)$ is contained in $H(F)_f$ and the diagram

$$\begin{tikzcd}
G(F)_f \arrow[r, "\varphi"] \arrow[d, "\log_{G(F)}"'] & H(F)_f \arrow[d, "\log_{H(F)}"] \\
\mathrm{Lie}(G(F)) \arrow[r, "\varphi_*"'] & \mathrm{Lie}(H(F))
\end{tikzcd}$$

commutes.

3.2. **Semistability.** In this section, K denotes an arbitrary field of characteristic 0. Let G be a commutative algebraic group defined over K and V a K-linear subspace of $\mathrm{Lie}(G)$. We recall the notion “semistable” which is due to Wüstholz (see [1, Chapter 6]). We associate with (G, V) the index

$$\tau(G, V) := \begin{cases} \dfrac{\dim V}{\dim G} & \text{if } \dim G > 0, \\ 1 & \text{otherwise.} \end{cases}$$

The pair (G, V) is called semistable (over K) if for any proper quotient $\pi : G \to H$ defined over K, we have $\tau(G, V) \leq \tau(H, \pi_*(V))$ where $\pi_* : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ is the tangent map induced by π.

Lemma 3.1. *If (G, V) is not semistable then there exists a proper quotient $\pi : G \to G'$ such that $(G', \pi_*(V))$ is semistable.*

Proof. For H an algebraic group defined over K and W a K-linear subspace of Lie(G), we say that $(H, W) \prec (G, V)$ if there is a proper quotient $\pi : G \to H$ defined over K such that $\pi_*(V) = W$ and $\tau(H, W) < \tau(G, V)$. Let Σ be the set defined by

$$\Sigma := \{(H, W); (H, W) \prec (G, V)\}.$$

Since (G, V) is not semistable the set Σ is non-empty. We observe that the set $\{\tau(H, W); (H, W) \in \Sigma\}$ is finite, and this shows that there is an element (G', V') in Σ such that

$$\tau(G', V') = \min_{(H,W)\in\Sigma} \tau(H, W).$$

Assume now that (G', V') is not semistable then there exists a proper quotient $\pi' : G' \to H$ defined over K such that

$$\tau(G', V') > \tau(H, \pi'_*(V')).$$

Since $(G', V') \prec (G, V)$ there is a proper quotient $\pi : G \to G'$ defined over K such that $\pi_*(V) = V'$. Let $q : G \to H$ be the composition of π' with π. Then q is also a proper quotient and

$$q_*(V) = (\pi' \circ \pi)_*(V) = \pi'_*(\pi_*(V)) = \pi'_*(V').$$

This shows that

$$\tau(H, q_*(V)) = \tau(H, \pi'_*(V')) < \tau(G', V') < \tau(G, V),$$

in other words $(H, q_*(V)) \in \Sigma$. It follows that

$$\tau(G', V') \leq \tau(H, q_*(V)) = \tau(H, \pi'_*(V)).$$

This contradicts the inequality $\tau(G', V') > \tau(H, \pi'_*(V'))$ above, and the lemma is proved. □

3.3. **p-adic Schwarz lemma.** For later use we quote the following proposition, which is a p-adic version of the Schwarz lemma. For any complete subfield F of $\mathbb{C}_p$ and for any real number $R \geq 0$ we set $B_F(R) := \{x \in F; |x|_p < R\}$ and $\overline{B}_F(R) := \{x \in F; |x|_p \leq R\}$; we will skip the subscript F when $F = \mathbb{C}_p$. Let $f(x) = \sum_n a_n x^n$ be an analytic function on $\overline{B}(r)$ with $r > 0$. We define $|f|_r := \sup_n |a_n|_p r^n = \max_n |a_n|_p r^n$. Then we have the following statement.

Lemma 3.2 (Proposition 3.3 in [6]). *Let $t \geq s$ be positive real numbers, q a positive integer, f an analytic function on $\overline{B}_F(t)$, and Γ a finite subset of $\overline{B}_F(s)$ of cardinality $l \geq 2$. We define*

$$\delta := \inf\{|\gamma - \gamma'|_p; \gamma, \gamma' \in \Gamma, \gamma \neq \gamma'\}$$

and

$$\mu := \sup\{|f^{(m)}(\gamma)|_p; m = 0, \ldots, q-1, \gamma \in \Gamma\}$$

with $f^{(m)}$ the m-th derivative of f. Put $r_p = p^{-\frac{1}{p-1}}$ and assume that $\delta \leq 1$. Then

$$|f|_s \leq \max\left\{\left(\frac{s}{t}\right)^{ql} |f|_t, \mu\left(\frac{s}{\delta}\right)^{ql-1} r_p^{-(q-1)}\right\}.$$

3.4. **Other preliminaries.** Let G be a commutative algebraic group defined over an algebraic number field K of dimension $n > 0$. It is known that G can be embedded into the projective space $\mathbb{P}^N$ with some positive integer N, so that G is realized biregularly as a quasi-projective subset of $\mathbb{P}^N$, and that this embedding can be chosen such that the group law $G \times G \to G$ extends to a regular action $G \times \overline{G} \to \overline{G}$ of G on $\overline{G}$ with $\overline{G}$ a compactification of G (see [8, Section 1.3] and [5, Section I-III], where explicit such embeddings using exponential- and Theta-functions are constructed). This allows one to associate to every element of the Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ an invariant vector field on $\overline{G}$ which induces a derivation from $\Gamma(U, \mathcal{O}_{\overline{G}})$ to itself; here U is the open affine subset in $\overline{G}$ defined by $\overline{G} \cap \{X_0 \neq 0\}$ with X_0 the first projective coordinate on $\mathbb{P}^N$

(for this we refer to [8, Section 1.3] or [9, Section 2]). Furthermore, the affine algebra $\Gamma(U, \mathcal{O}_{\overline{G}})$ is generated by $\xi_1, \dots, \xi_N$ over K, where

$$\xi_i := \left(\frac{X_i}{X_0}\right)\bigg|_U, \quad \forall i = 1, \dots, N$$

with $X_1, \dots, X_N$ the other projective coordinates on $\mathbb{P}^N$. This shows that $K[\xi_1, \dots, \xi_N]$ is stable under the action of any element in $\mathfrak{g}$. We call a map $L : \{1, \dots, n\} \to \mathfrak{g}$ a basis if $L(1), \dots, L(n)$ is a basis for $\mathfrak{g}$. It follows from above that the regular vector field $L(j)$ maps ξ_i to an element in $K[\xi_1, \dots, \xi_N]$ for any $i = 1, \dots, N$ and $j = 1, \dots, n$. In other words, there are polynomials $P_{i,L(j)}$ in N variables with coefficients in K such that

$$L(j)\xi_i = P_{i,L(j)}(\xi_1, \dots, \xi_N), \quad \forall i = 1, \dots, N, \forall j = 1, \dots, n.$$

This means that

$$\mathcal{L}_j := L(j)(\mathcal{O}_K[\xi_1, \dots, \xi_N])$$

is an $\mathcal{O}_K$-module in $K[\xi_1, \dots, \xi_N]$ for any $j = 1, \dots, n$. Put $\mathcal{L} = \mathcal{L}_1 + \cdots + \mathcal{L}_n$ and define

$$\mathcal{I}_L := (\mathcal{O}_K[\xi_1, \dots, \xi_N] : \mathcal{L}) = \{t \in \mathcal{O}_K; t\mathcal{L} \subset \mathcal{O}_K[\xi_1, \dots, \xi_N]\}.$$

Then $\mathcal{I}_L$ is an ideal of $\mathcal{O}_K$ and its norm $N_{K:\mathbb{Q}}(\mathcal{I}_L)$ is an ideal in $\mathbb{Z}$ which has to be principal. It takes the form (δ_L) for some positive integer δ_L. We call δ_L the denominator of L.

Denote by $\partial_1, \dots, \partial_n$ the canonical basis of $\mathrm{Lie}(K_v^n)$ defined as $\partial_i x_j = \delta_{ij}$ for all $i = 1, \dots, n$ and for all $j = 1, \dots, N$, where δ_{ij} are Kronecker's delta and x_i are the coordinate functions of K_v^n. We define the isomorphisms of K_v-vector spaces

$$\partial : K_v^n \to \mathrm{Lie}(K_v^n), \quad x = (x_1, \dots, x_n) \mapsto x_1\partial_1 + \cdots + x_n\partial_n$$

and

$$\iota : \mathrm{Lie}(K_v^n) \to \mathrm{Lie}(G(K_v)), \quad \iota(\partial_1) = L_1, \dots, \iota(\partial_n) = L_n.$$

We consider now the set $G(K_v)$ of K_v-points of G. It is known that $G(K_v)$ is a Lie group over K_v. By [3, Chapter III, §7], there is a map exp (which is called exponential map) defined and locally analytic on an open disk U_v of $G(K_v)$. The functions

$$f_i := \xi_i \circ \mathrm{Exp}, \quad i = 1, \dots, N$$

are analytic on $\Lambda_v := (\iota \circ \partial)^{-1}(U_v)$ in K_v^n, where $\mathrm{Exp} = \exp \circ \iota \circ \partial$ and satisfy

$$\partial_j(f_i) = L(j)(\xi_i) \circ \mathrm{Exp} = P_{i,L(j)}(\xi_1, \dots, \xi_N) \circ \mathrm{Exp} = P_{i,L(j)}(f_1, \dots, f_N)$$

for any $i = 1, \dots, N$ and $j = 1, \dots, n$. The map $f_L = (f_1, \dots, f_N) : \Lambda_v \to K_v^N$ is called the normalized analytic representation of the exponential map exp with respect to the basis L. We define

$$d_L := \max_{i,j} \deg P_{i,L(j)}; \quad e_L := v(\delta_L); \quad h_L := \max_{i,j} h(P_{i,L(j)})$$

and

$$\omega_L := \max\{1, e_L\}(h_L + \log \delta_L + \log d_L),$$

here by convention, $\log d_L = 0$ if $d_L = 0$.

We quote the following two statements from [6].

Lemma 3.3 (Lemma 3.8 in [6]). *Let $L : \{1, \dots, n\} \to \mathfrak{g}$ be a basis and $P(T_1, \dots, T_N)$ a polynomial in N variables with coefficients in K of total degree $\leq D$. Let T be a non-negative integer and $t = (t_1, \dots, t_n) \in \mathbb{Z}_{\geq 0}^n$ be such that $T = t_1 + \cdots + t_n$. There exists a polynomial $P_t \in K[T_1, \dots, T_N]$ such that*

$$\partial^t P(f_1, \dots, f_N) = P_t(f_1, \dots, f_N),$$

satisfying

1. $\deg P_t \leq D + T(d_L - 1)$,
2. $\log |P_t|_v \ll \log |P|_v + T(h_L + \log(D + Td_L)), \quad \forall v \in M_K$,

where $\partial^m := \partial_1^{m_1} \cdots \partial_k^{m_k}$ for $m = (m_1, \dots, m_k) \in \mathbb{Z}_{\geq 0}^k$ with $0 \leq k \leq n$.

Lemma 3.4 (Proposition 3.11 in [6])**.** *The functions f_i satisfy*

$$|f_i(x)|_p < 1, \quad \forall x \in B^n(|\delta_L|_p r_p).$$

4. Proofs

With notations as in Theorem 2.2, we put $n = \dim G$ and $k = \dim_{\overline{\mathbb{Q}}} V$.

4.1. **Choice of basis.** Since G is defined over $\overline{\mathbb{Q}}$, V is a $\overline{\mathbb{Q}}$-linear subspace of $\mathrm{Lie}(G)$ and since $\gamma \in G(\overline{\mathbb{Q}})$ there exists an algebraic number field K' such that G, V are defined over K' and such that $\gamma \in G(K')$. Let $\Gamma(\gamma) = \{\gamma^i; i \in \mathbb{Z}\}$ be the subgroup in $G(K')$ generated by γ.

Lemma 4.1. *There exists an embedding $\psi : G \to \mathbb{P}^N$ defined over a finite field extension of K' such that $\psi(e) = (1 : 0 : \ldots : 0)$ and $X_0(\psi(g)) \neq 0$ for all $g \in G(K')$; here e is the unity element of G.*

Proof. This is Lemma 4.1 in [6]; for the convenience of the reader we repeat the proof. Let $\varphi : G \to \mathbb{P}^N$ be an embedding as in Section 3.4. Without loss of generality, one may assume that $\varphi(e) = (1 : 0 : \ldots : 0)$. We choose a field extension K_1 of K' of degree $N + 1$ and a basis $\epsilon_0, \ldots, \epsilon_N$ of K_1 over K'. It is clear that the vectors

$$(\epsilon_0, 0, \ldots, 0), (-\epsilon_1, \epsilon_0, 0, \ldots, 0), \ldots, (-\epsilon_N, 0, \ldots, 0, \epsilon_0)$$

form a basis of K_1^{N+1} which gives rise to a unique element in $\mathrm{GL}_{N+1}(K_1)$ mapping this basis to the standard basis of K_1^{N+1}. This linear isomorphism is expressed explicitly by the matrix

$$A = \begin{pmatrix} \epsilon_0^{-1} & \epsilon_0^{-2}\epsilon_1 & \ldots & \epsilon_0^{-2}\epsilon_N \\ 0 & \epsilon_0^{-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \epsilon_0^{-1} \end{pmatrix}.$$

We let ψ be the composition of A with the embedding φ above. Then $\psi(e)$ has projective coordinates $(1 : 0 : \ldots : 0)$ and $X_0(\psi(g)) \neq 0$ for all $g \in G(K')$. Indeed, let $(x_0 : x_1 : \ldots : x_N)$ be a projective coordinate of $\varphi(g)$. By the construction of ψ, we obtain

$$\begin{aligned}\psi(g) &= (\epsilon_0^{-1}x_0 + \epsilon_0^{-2}\epsilon_1 x_1 + \cdots + \epsilon_0^{-2}\epsilon_N x_N : \epsilon_0^{-1}x_1 : \ldots : \epsilon_0^{-1}x_N) \\ &= (\epsilon_0 x_0 + \epsilon_1 x_1 + \cdots + \epsilon_N x_N : \epsilon_0 x_1 : \ldots : \epsilon_0 x_N).\end{aligned}$$

Thus we see that $\psi(e) = (1 : 0 : \ldots : 0)$. In addition, since $\epsilon_0, \ldots, \epsilon_N$ is a basis of K_1 over K' and $x_0, \ldots, x_N$ are in K', not all zero, it follows that $X_0(\psi(g))$ is non-zero. Note that the embedding ψ is defined over K_1. □

Lemma 4.2. *There are bihomogeneous polynomials $E_0, \ldots, E_N$ of bidegree (a, a) with coefficients in a finite field extension of K' and a Zariski open subset $U \subseteq G \times G$ containing $\Gamma(\gamma) \times \Gamma(\gamma)$ such that for $(g, g') \in U$ the homogeneous coordinates of $g + g'$ are*

$$(E_0(g, g') : \ldots : E_N(g, g')).$$

With such $E_1, \ldots, E_N$, we call $E = (E_1, \ldots, E_N)$ an addition formula for G.

Proof. This follows by [9, Section 2]. □

These two lemmas mean that there exists an algebraic number field K which contains K' and satisfies the following properties: There is an embedding over K of G into $\mathbb{P}^N$ such that the projective coordinate of the unity element of G is $(1 : 0 : \ldots : 0)$ and such that the first projective coordinate $X_0(\gamma')$ for all γ' in $\Gamma(\gamma)$ is non-zero, and there is an addition formula $E = (E_1, \ldots, E_N)$ with coefficients in K of G.

Our discussion has shown that we may assume the group G, the Lie algebra $\mathfrak{g} := \mathrm{Lie}(G)$, the vector space V and the addition formula E are defined over K. The inclusion $K \subset \overline{\mathbb{Q}} \subset \mathbb{C}_p$ induces a non-archimedean valuation v on K dividing p. Denote by K_v the completion of K with respect to v, then K_v is a complete subfield of $\mathbb{C}_p$.

We fix a basis L of $\mathfrak{g}$ and let $f_L = (f_1, \dots, f_N)$ be the normalized analytic representation of the exponential map $\exp_{G(K_v)}$ with respect to L. We identify $\mathfrak{g}$ with K^n (by means of the basis L) and consider V as a K-linear subspace of K^n. It is possible to find a basis $e_1, \dots, e_k$ for V such that

$$e_i = (x_{i1}, \dots, x_{in}) \in \mathcal{O}_K^n, \quad \forall i = 1, \dots, k.$$

We also fix a positive integer α large enough such that $r := p^{-\alpha} < |\delta_L|_p r_p$ with $r_p := p^{-\frac{1}{p-1}}$ and such that the ball $B^n(r) := \{x = (x_1, \dots, x_n) \in \mathbb{C}_p^n ; |x_i|_p < r, \forall i = 1, \dots, n\}$ is contained in the domain of the map Exp. The functions $f_1, \dots, f_N$ are analytic in $B^n(r)$ and by Lemma 3.4 satisfy

$$|f_i(x)|_p < 1, \quad \forall x \in B^n(r), \quad \forall i = 1, \dots, N.$$

This gives the corresponding differential operators

$$\Delta_i = x_{i1}\partial_1 + \cdots + x_{in}\partial_n$$

in $\mathrm{Lie}(K^n)$ with $\partial_1, \dots, \partial_n$ the canonical basis of $\mathrm{Lie}(K_v^n)$. Put

$$b := \max\{h(x_{ij}); 1 \le i \le k, 1 \le j \le n\}, \quad B := e^b,$$

where h denotes the (Weil) logarithmic height. Define d as the degree of the extension of K over $\mathbb{Q}$. From now on for each $t = (t_1, \dots, t_k) \in \mathbb{Z}_{\ge 0}^k$ we write $\Delta^t = \Delta_1^{t_1} \cdots \Delta_k^{t_k}$ and for each $t = (t_1, \dots, t_m) \in \mathbb{Z}^m$ we write $|t| = t_1 + \cdots + t_m$.

4.2. **The auxiliary function.** Let P be a polynomial in $N+1$ variables $X_0, \dots, X_N$ in $\mathbb{C}_p[X_0, \dots, X_N]$. We associate with P the analytic function $\Phi_P : B^n(r) \to \mathbb{C}_p$ which is given by

$$\Phi_P(x) := P(1, f_1(x), \dots, f_N(x)), \quad \forall x \in B^n(r).$$

Let $g \in G(K_v)$ be defined by $g = \mathrm{Exp}(x)$ with $x \in B^n(r)$. We define the order of P at g along V to be infinity, if Φ_P is identically zero in a neighborhood of x, and to be the order of Φ_P at x along $V_{K_v} := V \otimes_K K_v$, otherwise (we refer the reader to Section 3.6 in [6] for more detailed description). Since $\gamma \in G(K_v)_f$ and since $\mathrm{Exp}(B(r))$ is an open subgroup in $G(K_v)_f$ there is a positive integer m such that $\gamma^m \in \mathrm{Exp}(B(r))$. In order to prove Proposition 2.5, we may therefore assume that $\gamma \in \mathrm{Exp}(B(r))$. Let u be the element of $B(r)$ such that $\mathrm{Exp}(u) = \gamma$ and put $h := \max\{1, h(\gamma)\}$. Throughout this paper, constants do not depend on b, h and p and we also write $A \ll B$ (resp. $A \gg B$) if there is a positive constant c such that $A \le cB$ (resp. $A \ge cB$). Let S_0, D, T be positive integers. We use the notations $c_1, c_2, ...$ for real positive constants which are independent of b, h and p. Denote by $h(P)$ the height of the polynomial P. We get the following proposition. We remark that the proof will be similar to that of [6, Proposition 4.2], but it will be simpler because the additive group $\mathbb{G}_a$ does not appear.

Proposition 4.3. *There are positive constants c_1 and c_2 such that if $D^n \ge c_1 S_0 T^k$ there is a homogeneous polynomial P in $X_0, \dots, X_N$ of degree D with coefficients in $\mathcal{O}_K$ such that*

1. *P does not vanish identically on G,*
2. *$(\Delta^t \Phi_P)(su) = 0, \forall 0 \le s < S_0, \forall t = (t_1, \dots, t_k) \in \mathbb{Z}_{\ge 0}^k, t_1, \dots, t_k < 2T$,*
3. *$h(P) \le c_2\big(T(h_L + \log \delta_L + \log(D + T \log d_L) + b) + DS_0^2 h\big)$.*

Proof. Since the dimension of G is n, without loss of generality, we may assume that the homogeneous coordinates $X_0, \dots, X_n$ are algebraically independent modulo the ideal of G. We shall construct a non-zero homogeneous polynomial P in $n+1$ variables $X_0, \dots, X_n$ of degree D (this polynomial therefore satisfies 1. in the proposition) such that 2. and 3. in the proposition are also satisfied. We write

$$P(X) = P(X_0, \dots, X_n) = \sum_{i=1}^{D_1} p_i M_i(X_0, \dots, X_n),$$

where $M_1, \ldots, M_{D_1}$ run through all homogeneous monomials of degree D in $n+1$ variables $X_0, \ldots, X_n$. Let $E = (E_1, \ldots, E_N)$ be the addition formula for G given in Section 4.1. By abuse of notation we put

$$E_i(z,x) := E_i(1, f_1(z), \ldots, f_N(z), 1, f_1(x), \ldots, f_N(x)),$$

for z, x in $B^n(r)$ and define

$$\Phi_s(x) := \Phi_P(su + x) E_0(su, x)^D.$$

For $I := \{(s,t); 0 \le s < S_0, t = (t_1, \ldots, t_k), 0 \le t_1, \ldots, t_k < 2T\}$, we shall determine coefficients p_i such that

$$(\Delta^t \Phi_s)(0) = 0, \quad \forall (s,t) \in I.$$

We express $\Phi_s(x)$ as

$$\Phi_s(x) = \Phi_P(su + x) E_0(su, x)^D = \sum_i p_i Q_{i,s}(f_1(x), \ldots, f_N(x))$$

for polynomials $Q_{i,s}$ in N variables with the property that there are positive integers $\mathrm{d}_s \ll s^2 h$ such that

$$\text{(1)} \qquad \mathrm{d}_s {\delta_L}^{|m|} \big(\partial^m Q_{i,s}(f_1, \ldots, f_N)\big)(0) \in \mathcal{O}_K$$

and

$$\text{(2)} \qquad \log \Big| \Big(\partial^m (Q_{i,s}(f_1, \ldots, f_N)\Big)(0) \Big|_v \ll |m|(h_L + \log(D + |m| d_L)) + Ds^2 h$$

for any $m = (m_1, \ldots, m_n) \in \mathbb{Z}_{\ge 0}^n$ and for any $v \in M_K$, where ∂^m denotes the differential operator $\partial_1^{m_1} \cdots \partial_n^{m_n}$ and M_K denotes the set of all places on K. For $i = 1, \ldots, D_1$ and $(s,t) \in I$ we expand

$$\begin{aligned} a_i^{st} : &= \big(\Delta^t (Q_{i,s}(f_1, \ldots, f_N))\big)(0) \\ &= \big(\Delta_1^{t_1} \cdots \Delta_k^{t_k} (Q_{i,s}(f_1, \ldots, f_N))\big)(0) \\ &= \Big(\prod_{i=1}^k (x_{i1}\partial_1 + \cdots + x_{in}\partial_n)^{t_i} (Q_{i,s}(f_1, \ldots, f_N))\Big)(0) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_{|t|}=1}^n x_{i_1,j_1} \cdots x_{i_{|t|},j_{|t|}} \partial_{j_1} \cdots \partial_{j_{|t|}} (Q_{i,s}(f_1, \ldots, f_N))\big)(0), \end{aligned}$$

with $(i_1, \ldots, i_{|t|}) = (1, \ldots, 1, 2, \ldots, 2, \ldots, k, \ldots, k)$ where ι repeats t_ι times for $\iota = 1, \ldots, k$. By (2) we obtain

$$\log \Big| \Big(\partial_{j_1} \cdots \partial_{j_{|t|}} (Q_{j,s}(f_1, \ldots, f_N))\Big)(0) \Big|_v \ll T(h_L + \log(D + T d_L)) + Ds^2 h$$

which, together with the inequalities

$$\sum_{j_1=1}^n \cdots \sum_{j_{|t|}=1}^n \Big| x_{i_1,j_1} \cdots x_{i_{|t|},j_{|t|}} \Big|_v \le \prod_{i=1}^k \Big(\sum_{j=1}^n |x_{ij}|_v \Big)^{t_i} \le (nB)^{|t|}, \quad \forall v \in M_K,$$

gives

$$\log |a_i^{st}|_v \ll T(h_L + \log(D + T d_L) + b) + Ds^2 h.$$

Combining this with (1), we see that $\mathrm{d}_s {\delta_L}^{2nT} a_i^{st}$ is in $\mathcal{O}_K$ and

$$\log |\mathrm{d}_s {\delta_L}^{2nT} a_i^{st}|_v \ll T(\log \delta_L + h_L + \log(D + T \log d_L) + b) + DS_0^2 h$$

for $(s,t) \in I$ and for $v \in M_K^\infty$. We now consider the linear forms

$$l_{st} := \sum_{i=1}^{D_1} b_i^{st} T_i$$

in $n_0 := D_1 = \binom{D+n}{n}$ variables, where $b_i^{st} := \mathrm{d}_s {\delta_L}^{2nT} a_i^{st}$ for $(s,t) \in I$. The number m_0 of these linear forms satisfies $m_0 \ll S_0 T^k$. Since $b_i^{st} \in \mathcal{O}_K$ we get

$$\sum_{v \in M_K^\infty} \log \max_i |b_i^{st}|_v \ll T(h_L + \log \delta_L + \log(D + T \log d_L) + b) + DS_0^2 h.$$

We now apply Siegel's lemma (cf. [2, Corollary 11]). It follows that under the condition $D^n \gg S_0 T^k$ there is a non-zero vector $p_0 = (p_i)$ with coordinates in $\mathcal{O}_K$ such that $l_{st}(p_0) = 0$ for all $(s,t) \in I$ and such that

$$h(P) \ll T(h_L + \log \delta_L + \log(D + T d_L) + b) + DS_0^2 h.$$

It remains to show that $(\Delta^t \Phi_P)(su) = 0$. In fact, since $l_{st}(p_0) = 0$ one gets $(\Delta^t \Phi_s)(0) = 0$ for $(s,t) \in I$. Put

$$\Phi_s^*(x) := \Phi_P(su + x), \quad E_s(x) := E_0(su, x)^D$$

then $\Phi_s^* = \Phi_s E_s^{-D}$. We therefore deduce by Leibniz' rule for derivations that

$$(\Delta^t \Phi_P)(su) = (\Delta^t \Phi_s^*)(0) = \big(\Delta^t(\Phi_s E_s^{-D})\big)(0) = 0.$$

This completes the proof. □

Proposition 4.4. *Let S be a positive integer and s an integer such that $0 \le s < S$. Let P be a polynomial determined as in the above Proposition. Assume that Φ has a zero at su of exact order T' along $\mathscr{W}$ for some positive integer T'. Let t be any element in $\mathbb{Z}_{\ge 0}^k$ with $|t| = T'$ such that $(\Delta^t \Phi_P)(su) \neq 0$, then*

$$\log |(\Delta^t \Phi_P)(su)|_p > -c_3(T'(h_L + \log \delta_L + \log(D + T' d_L) + b) + DS^2 h)$$

for some positive constant c_3.

Proof. We define

$$\Phi_s^*(x) := \Phi_P(su + x), \quad E_s(x) := E_0(su, x), \quad \Phi_s(y, x) := \Phi_s^*(y, x) E_s(x)^D.$$

By our assumption

$$0 = (\Delta^\tau \Phi_P)(su) = (\Delta^\tau \Phi_P)(su) = (\Delta^\tau \Phi_s^*)(0)$$

for $\tau \in \mathbb{Z}_{\ge 0}^n$ with $|\tau| < T'$ and Leibniz' rule gives

$$(\Delta^\tau \Phi_s)(0) = \big(\Delta^\tau(\Phi_s^* E_s^D)\big)(0) = 0.$$

Using Leibniz' rule again, one gets

$$(\Delta^t \Phi_P)(su) = \big(\Delta^t(\Phi_s E_s^{-D})\big)(0) = (\Delta^t \Phi_s)(0) E_s^{-D}(0).$$

The same arguments as in the proof of Proposition 4.3 (just replace S_0 by S) show that

$$h((\Delta^t \Phi_s)(0,0)) \ll T'(h_L + \log \delta_L + \log(D + T' \log d_L) + b) + DS^2 h.$$

Furthermore

$$h(E_s^{-D}(0)) = h(E_0(su, 0)^{-D}) = Dh(E_0(su, 0)) \ll DS^2 h.$$

Since $(\Delta^t \Phi_P)(su) \neq 0$, Liouville's inequality gives

$$\begin{aligned}\log |(\Delta^t \Phi_P)(su)|_p &\gg -h((\Delta^t \Phi_P)(su)) = -h\big((\Delta^t \Phi_s)(0) E_s(0)^{-D}\big) \\ &\gg -\big(T'(h_L + \log \delta_L + \log(D + T' d_L) + b) + DS^2 h\big),\end{aligned}$$

and the proposition follows. □

4.3. **Proof of Proposition 2.5.** Assume on the contrary that $\log_{G(F)}(\gamma) \in V_F$. Since K_v is a subfield of F it follows that

$$\log_{G(F)}(\gamma) = \log_{G(K_v)}(\gamma) \in \mathrm{Lie}(G(K_v)).$$

This means that $\log_{G(K_v)}(\gamma)$ is an element in

$$V_F \cap \mathrm{Lie}(G(K_v)) = \big(V \otimes_K F\big) \cap (\mathfrak{g} \otimes_K K_v) = V \otimes_K K_v.$$

In other words the element u belongs to the K_v-vector space generated by the basis $e_1, \dots, e_k$. We express u in terms of this basis and get

$$u = (u_1, \dots, u_n) = w_1 e_1 + \cdots + w_k e_k$$

for $w_1, \dots, w_k \in K_v$. By Section 4.1, we write $e_j = (x_{j1}, \dots, x_{jn})$ for $j = 1, \dots, n$ and calculate that

$$u = \sum_{j=1}^{k} w_j (x_{j1}, \dots, x_{jn}) = \Big(\sum_{j=1}^{k} w_j x_{j1}, \dots, \sum_{j=1}^{k} w_j x_{jn} \Big)$$

which means that

$$u_i = \sum_{j=1}^{k} w_j x_{ji}, \quad \forall i = 1, \dots, n.$$

Let c be a sufficiently large positive constant and let $[x]$ denote the largest integer less than or equal to x. Let ω_L be the quantity defined in Section 3.4. We choose

$$\begin{aligned} S_0 &= [c\omega_L b \log h], \\ S &= [c^2 S_0], \\ D &= \Big[c^{\frac{5d+1}{n-d}} S_0^{\frac{n+1}{n-d}} h^{\frac{d}{n-d}} \Big], \\ T &= \Big[c^{\frac{4d+n+1}{n-d}} S_0^{\frac{n+1}{n-d}} h^{\frac{n}{n-d}} \Big]. \end{aligned}$$

Our parameters satisfies $D^n \geq c_1 S_0 T^k$. Hence, there exists a polynomial P with properties as in Proposition 4.3 which we express as $P = \sum_i p_i M_i$ with M_i monomials in $N+1$ variables. We write Φ instead of Φ_P. For $t = (t_1, \dots, t_k) \in \mathbb{Z}_{\geq 0}^k$ such that $|t| < T$ we define the analytic function

$$f(z) := (\Delta^t \Phi)(zu)$$

in the variable $z \in B(r)$. For $0 \leq \tau < T$ we apply the composition rule for derivatives and get

$$f^{(\tau)}(z) = \big((u_1 \partial_1 + \cdots + u_n \partial_n)^\tau \Delta^t \Phi\big)(zu).$$

We use the representations

$$u_i = \sum_{j=1}^{k} w_j x_{ji}, \quad \forall i = 1, \dots, n$$

to write

$$\sum_{i=1}^{n} u_i \partial_i = \sum_{i=1}^{n} \Big(\sum_{j=1}^{k} w_j x_{ji} \Big) \partial_i = \sum_{j=1}^{k} w_j \Big(\sum_{i=1}^{n} x_{ji} \partial_i \Big) = \sum_{j=1}^{k} w_j \Delta_j.$$

This leads to

$$f^{(\tau)}(z) = \big((w_1 \Delta_1 + \cdots + w_k \Delta_k)^\tau \Delta^t \Phi\big)(zu).$$

Applying multinomial expansion and Proposition 4.3 one gets

$$f^{(\tau)}(s) = 0, \quad \forall 0 \leq s < S_0.$$

Define $\overline{B}(R) := \{x \in \mathbb{C}_p; |x|_p \leq R\}$, we shall show that f is analytic in $\overline{B}(R)$ for $R := p^{\frac{1}{2d}}$. To prove this, we observe that $v(K_v) = (1/d_v)\mathbb{Z}$ with $d_v := [K_v : \mathbb{Q}_p]$. This means that

$$v(u_i) = \frac{a_i}{d_v},$$

for some $a_i \in \mathbb{Z}_{\geq 0}$. Since $u \in B^n(r)$ it follows that $v(u_i) - \alpha > 0$, i.e. $a_i - d_v\alpha > 0$. This together with the inequality $d = [K : \mathbb{Q}] \geq [K_v : \mathbb{Q}_p] = d_v$ implies that

$$v(u_i) - \alpha = \frac{a_i - d_v\alpha}{d_v} \geq \frac{1}{d_v} \geq \frac{1}{d}.$$

Hence

$$R|u_i|_p = p^{\frac{1}{2d}} p^{-v(u_i)} = p^{-\frac{1}{2d}} p^{-(v(u_i)-\alpha-\frac{1}{d})} p^{-\alpha} < p^{-\alpha} = r.$$

This shows that $zu \in B^n(r)$ for any $z \in \overline{B}(R)$. In particular, the function f is analytic in $\overline{B}(R)$. This means that there is a power series $\sum_{n\geq 0} a_n x^n$ which is convergent in $\overline{B}(R)$ such that $f(x) = \sum_{n\geq 0} a_n x^n$ for any $x \in \overline{B}(R)$. As usual for each $\kappa \in [0, R]$ we put

$$|f|_\kappa = \sup_{n\geq 0} |a_n|_p^n \kappa^n.$$

Define $R_i(x) := M_i(1, f_1(x), \ldots, f_N(x))$. We have

$$\begin{aligned} f(z) &= (\Delta^t\Phi)(zu) \\ &= \sum_i p_i\big(\Delta_1^{t_1} \cdots \Delta_k^{t_k} R_i\big)(zu) \\ &= \sum_i p_i\big((x_{11}\partial_1 + \cdots + x_{1n}\partial_n)^{t_1} \cdots (x_{k1}\partial_1 + \cdots + x_{kn}\partial_n)^{t_k} R_i\big)(zu) \end{aligned}$$

for $z \in \overline{B}(R)$. By multinomial expansion again and by the ultrametric inequality one gets

$$|f(z)|_p \leq \max_i \max_{|t|<T} |(\Delta^t R_i)(zu)|_p.$$

On the other hand, Lemma 3.3 tells us that

$$(\Delta^t R_i)(zu) = Q_i(f_1(zu), \ldots, f_N(zu))$$

for polynomials Q_i in N variables such that ${\delta_L}^T Q_i$ have coefficients in $\mathcal{O}_K$. Since $zu \in B(r)$ from Section 4.1 we have $|f_i(zu)|_p < 1$ for $i = 1, \ldots, N$. Hence

$$|(\Delta^t R_i)(zu)|_p \leq |{\delta_L}^{-1}|_p^T$$

which means that

$$|f(z)|_p \leq |{\delta_L}^{-1}|_p^T, \quad \forall z \in \overline{B}(R).$$

In other words $|f|_R \leq |{\delta_L}^{-1}|_p^T$. We now apply Lemma 3.2 to the function f to get

$$|f|_1 \leq p^{-\frac{1}{2d}S_0T}|f|_R \leq |{\delta_L}^{-1}|_p^T p^{-\frac{1}{2d}S_0T}.$$

Hence

$$|(\Delta^t\Phi)(su)|_p = |f(s)|_p \leq |f|_1 \leq |{\delta_L}^{-1}|_p^T p^{-\frac{1}{2d}S_0T}.$$

This leads to

$$\log|(\Delta^t\Phi)(su)|_p \ll -T\log|\delta_L|_p - S_0T\log p = -(S_0 - e_L)T\log p \tag{3}$$

for any $t \in \mathbb{Z}_{\geq 0}^d$ such that $|t| < T$. We shall show that the order of P along V at any point γ^s with $0 \leq s < S$ is at least T. In fact, assume that it is not true at some point γ^{s_0} with $0 \leq s_0 < S$, then by definition the exact order of Φ at s_0u along V_v is $T_0 < T$, i.e. there is a k-tuple $t_0 \in \mathbb{Z}_{\geq 0}^k$ such that $|t_0| = T_0$ and $(\Delta^{t_0}\Phi)(s_0u) \neq 0$. By Proposition 4.4 one has

$$\log|(\Delta^{t_0}\Phi)(su)|_p \gg -(T_0(h_L + \log\delta_L + \log(D + T_0d_L) + b) + DS^2h).$$

Combining this with (3) we get

$$T(S_0 - e_L)\log p \ll (T_0(h_L + \log\delta_L + \log(D + T_0d_L) + b) + DS^2h).$$

This cannot hold if c is large enough. Therefore Φ vanishes at any point of the set $\{su; 0 \leq s < S_0\}$ of order at least T along V. By the assumption (G, V) is semistable and therefore [1, Theorem 6.14] implies that there exists an integer s' such that $0 < s' < S$ and $\gamma^{s'} = e$, i.e. γ is a torsion point, a contradiction. This ends the proof.

4.4. **Proof of Theorem 2.2.** The proof of Theorem 2.2 is done by induction on $\dim G$. If $\dim G = 1$ then V must be equal to $\mathrm{Lie}(G)$, and we choose $H = G$. Now we assume that $\dim G > 1$. By Proposition 2.5 we see that (G, V) is not semistable. Lemma 3.1 shows that there is a proper quotient $\pi : G \to G'$ such that (G', V') is semistable, where $V' = \pi_*(V)$. Let $\pi_F : G(F) \to G'(F)$ be the F-analytic homomorphism induced by π. It is known that the differential map $(\pi_F)_* = \pi \otimes_{\overline{\mathbb{Q}}} \mathrm{id}_F$. By Section 3.1 we have that the following diagram

$$\begin{tikzcd}
G(F)_f \arrow[r, "\pi_F"] \arrow[d, "\log_{G(F)}"'] & G'(F)_f \arrow[d, "\log_{G'(F)}"] \\
\mathrm{Lie}(G(F)) \arrow[r, "(\pi_F)_*"'] & \mathrm{Lie}(G'(F))
\end{tikzcd}$$

commutes, it follows that

$$\log_{G'(F)}(\pi_F(\gamma)) = (\pi_F) * \left(\log_{G(F)}(\gamma)\right) \in (\pi_F) * (V \otimes_{\overline{\mathbb{Q}}} F) = \pi_*(V) \otimes_{\overline{\mathbb{Q}}} F = V' \otimes_{\overline{\mathbb{Q}}} F.$$

By Proposition 2.5 again we conclude that $\log_{G'(F)}(\pi_F(\gamma))$ must be 0, this is equivalent to $\pi_F(\gamma)$ being a torsion point. Let m be the order of $\pi_F(\gamma)$ and define $\widetilde{G} := \ker \pi$. Then $\widetilde{G}$ is a commutative algebraic group defined over $\overline{\mathbb{Q}}$ and $\gamma^m \in \widetilde{G}(\overline{\mathbb{Q}})$ (since $\gamma \in G_f(\overline{\mathbb{Q}})$). Therefore

$$\log_{\widetilde{G}(F)}(\gamma^m) \in \mathrm{Lie}(\widetilde{G}(F)) = \mathrm{Lie}(\widetilde{G}) \otimes_{\overline{\mathbb{Q}}} F$$

and

$$\log_{\widetilde{G}(F)}(\gamma^m) = \log_{G(F)}(\gamma^m) = m \log_{G(F)}(\gamma) \in V \otimes_{\overline{\mathbb{Q}}} F.$$

This gives

$$\log_{\widetilde{G}(F)}(\gamma^m) \subseteq (V \cap \mathrm{Lie}(\widetilde{G})) \otimes_{\overline{\mathbb{Q}}} F.$$

Furthermore we see that $\gamma^m \in \widetilde{G}(F)_f$. Since π is proper it follows that the dimension of $\widetilde{G}$ is positive. We apply the inductive hypothesis to the commutative algebraic group $\widetilde{G}$, the algebraic point γ^m and the $\overline{\mathbb{Q}}$-linear subspace $V \cap \mathrm{Lie}(\widetilde{G})$ of $\mathrm{Lie}(\widetilde{G})$ to obtain an algebraic subgroup $\widetilde{H}$ of $\widetilde{G}$ of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\gamma^m \in \widetilde{H}(\overline{\mathbb{Q}})$ and such that $\mathrm{Lie}(\widetilde{H}) \subseteq \mathrm{Lie}(\widetilde{G}) \cap V \subseteq V$. Finally we take H such that $H(\overline{\mathbb{Q}}) := \{\alpha \in G(\overline{\mathbb{Q}}); \alpha^m \in \widetilde{H}(\overline{\mathbb{Q}})\}$. Then H is an algebraic subgroup of G of positive dimension defined over $\overline{\mathbb{Q}}$ and $\gamma \in H(\overline{\mathbb{Q}})$ and, in addition, $\mathrm{Lie}(H) \subseteq V$. This concludes the proof.

4.5. **Proof of Corollary 2.3.** The F-vector space $W \otimes_{\overline{\mathbb{Q}}} F$ is a subspace of $\mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} F$. In particular, $\dim_{\overline{\mathbb{Q}}} W = \dim_F(W \otimes_{\overline{\mathbb{Q}}} F)$ is finite. If T contains only torsion points then the map $\log_{G(F)}$ vanishes on T. This means that W is trival, and we choose $H = \{e\}$. Otherwise there exist a positive integer m and non-torsion elements $\gamma_1, \ldots, \gamma_m$ in T such that $\log_{G(F)}(\gamma_1), \ldots, \log_{G(F)}(\gamma_m)$ is a $\overline{\mathbb{Q}}$-basis for W. We apply successively Theorem 2.2 with $\gamma = \gamma_i$, and obtain algebraic subgroups H_i of G defined over $\overline{\mathbb{Q}}$ such that $\gamma_i \in H_i$ and $\mathrm{Lie}(H_i) \subseteq W$ for $i = 1, \ldots, m$. Let $H = H_1 \cdots H_m$ be the product of $H_1, \ldots, H_m$. This is an algebraic subgroup of G defined over $\overline{\mathbb{Q}}$ since G is commutative with

$$\mathrm{Lie}(H) = \mathrm{Lie}(H_1) + \cdots + \mathrm{Lie}(H_m).$$

Hence $\mathrm{Lie}(H)$ is a $\overline{\mathbb{Q}}$-vector subspace of W. On the other hand

$$\log_{G(F)}(\gamma_i) = \log_{H_i(F)}(\gamma_i) \in \mathrm{Lie}(H_i(F)) = \mathrm{Lie}(H_i) \otimes_{\overline{\mathbb{Q}}} F \subseteq \mathrm{Lie}(H) \otimes_{\overline{\mathbb{Q}}} F$$

for $i = 1, \ldots, m$ and this implies that $W \otimes_{\overline{\mathbb{Q}}} F \subseteq \mathrm{Lie}(H) \otimes_{\overline{\mathbb{Q}}} F$. We conclude that

$$\dim_{\overline{\mathbb{Q}}} \mathrm{Lie}(H) = \dim_{\overline{\mathbb{Q}}} W,$$

i.e. $\mathrm{Lie}(H) = W$. This proves the corollary.

4.6. **Proof of Corollary 2.4.** By Section 3.1 we have that the following diagram

$$\begin{tikzcd}
X(F)_f \arrow[r, "\varphi_F"] \arrow[d, "\log_{X(F)}"'] & G(F)_f \arrow[d, "\log_{G(F)}"] \\
\mathrm{Lie}(X(F)) \arrow[r, "(\varphi_F)_*"'] & \mathrm{Lie}(G(F))
\end{tikzcd}$$

is commutative. This gives

$$\begin{aligned}\log_{G(F)}(\varphi_F(x)) &= (\varphi_F)_*(\log_{X(F)}(x)) \subseteq (\varphi_F)_*(\mathrm{Lie}X(F)) \\ &= (\varphi_F)_*(\mathrm{Lie}(X) \otimes_{\overline{\mathbb{Q}}} F) = \varphi_*(\mathrm{Lie}(X)) \otimes_{\overline{\mathbb{Q}}} F.\end{aligned}$$

The corollary therefore follows from Theorem 2.2.

5. Acknowledgments

The authors are most grateful to Professor G. Wüstholz for very insightful discussions and for constant encouragement to work on the topic. Moreover, they are grateful to an anonymous referee for many helpful remarks. The first author was supported by Austrian Science Fund (FWF): P24574. The second author was supported by grant PDFMP2_122850 funded by the Swiss National Science Foundation (SNSF).

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, New Mathematics Monographs, vol. **9**, Cambridge University Press, 2007.

[2] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11-32.

[3] N. Bourbaki, *Elements of Mathematics. Lie groups and Lie algebras. Part I: Chapters* **1-3**. *English translantion.,* Actualities scientifiques et industrielles, Herman. Adiwes International Series in Mathematics. Paris: Hermann, Publishers in Arts and Science; Reading, Mass.: Addison-Wesley Publishing Company. XVII, 1975.

[4] D. Bertrand, *Lemmes de zèros et nombres transcendants*, Séminaire Bourbaki Vol. 1985/86, Astérisque **145-146** (1987), 21-44.

[5] G. Faltings and G. Wüstholz, *Einbettungen kommutativer algebraischer Gruppen und einige Eigenschaften*, J. Reine Angew. Math. **354** (1984), 175-205.

[6] C. Fuchs and D. H. Pham, *Commutative algebraic groups and p-adic linear forms*, http://arxiv.org/pdf/1404.4209v1.pdf.

[7] T. Matev, *The p-adic analytic subgroup theorem and applications*, http://arxiv.org/pdf/1010.3156v1.pdf.

[8] J. P. Serre, *Quelques propriétés des groupes algébriques commutatifs*, Astérisque **69-70**, 1979.

[9] G. Wüstholz, *Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen*, Ann. of Math. **129** (1989), 501-517.

[10] Y. G. Zarhin, *p-adic abelian integrals and commutative Lie groups*, J. Math. Sci. **81** (1996), no. 3, 2744-2750.

Clemens Fuchs
Department of Mathematics
University of Salzburg
Hellbrunnerstr. 34
5020 Salzburg
Austria
Email: clemens.fuchs@sbg.ac.at

Duc Hiep Pham
Department of Mathematics
Hanoi National University of Education
136 Xuan Thuy, Cau Giay, Hanoi
Vietnam
Email: phamduchiepk6@gmail.com